Claims

What is claimed is:

1. A system of establishing a secure link among multiple users on a single machine with a remote machine, comprising:

a subsystem to filter traffic so that traffic from each user is separate;

wherein the subsystem generates and associates a Security Association (SA) with at least one filter corresponding to the user and the traffic and employs the SA to establish the secure link.

2. The system of claim 1 being located on the single machine.

3. The system of claim 1 being located on the remote machine.

4. The system of claim 1, wherein the subsystem further comprises an Internet Key Exchange module and a policy module to generate and associate the security association.

5. The system of claim 4, wherein the policy module is configured *via* Internet Protocol Security (IPSEC).

6. The system of claim 5, wherein filters are provided from the policy module in order to filter traffic associated with the single machine and the remote machine.

7. The system of claim 6, wherein the single machine filter is associated with a communications port on the single machine.

8. The system of claim 7, wherein the remote machine determines filters dynamically to communicate with the filters associated with the single machine.

9. The system of claim 4, wherein the IKE module is adapted to provide User Mode negotiations in order to establish a secure link among the users.

10. The system of claim 9, wherein the User Mode negotiations utilize keying material derived from Main Mode negotiations in order to provide the secure link among users.

11. The system of claim 10, wherein the User Mode enables a plurality of Quick Mode negotiations in order to provide the secure link among users.

12. The system of claim 11, wherein the User Mode negotiation further comprises an initiator packet including at least one of a user identification initiator, a security association attribute, a nonce initiator, a proxy source, and a proxy destination.

13. The system of claim 12, wherein the initiator packet further comprises a user identification responder.

14. The system of claim 11, wherein the User Mode negotiation further comprises a responder packet including at least one of a user identification responder, a security association attribute, and a nonce responder.

15. The system of claim 11, wherein the User Mode enables a plurality of authentication packets to be sent to authenticate among users.

16. A system of establishing a secure link between a first machine and multiple services on a second machine, comprising:

a subsystem to filter traffic so that traffic from each service is separate;

wherein the subsystem generates and associates a Security Association (SA) with at least one filter corresponding to the user and the service and employs the SA to establish the secure link.

17. The system of claim 16, wherein the subsystem further comprises an Internet Key Exchange module and a policy module to generate and associate the security association.

18. The system of claim 17, wherein the policy module is configured *via* Internet Protocol Security (IPSEC).

19. The system of claim 18, wherein filters are provided from the policy module in order to filter traffic associated with the first machine and the second machine.

20. The system of claim 19, wherein the first machine filter is associated with a communications port on the first machine.

21. The system of claim 20, wherein the second machine determines filters dynamically to communicate with the filters associated with the first machine.

22. The system of claim 4, wherein the IKE module is adapted to provide User Mode negotiations in order to establish a secure link between the services.

23. The system of claim 22, wherein the User Mode negotiation further comprises an initiator packet including at least one of a user identification initiator, a security association attribute, a nonce initiator, a proxy source, and a proxy destination.

24. The system of claim 23, wherein multiple services are authenticated on the second machine by utilizing a policy look-up associated with service information relating to the initiator packet.

25. The system of claim 24, wherein if a multiple service authentication fails, the second machine initiates a User Mode negotiation.

26. A method of establishing a secure link among multiple users on a single machine with a remote machine, comprising the steps of:

filtering traffic so that traffic from each user is separate;

negotiating and authenticating a Security Association (SA) with at least one filter corresponding to the user and the traffic; and

employing the SA to establish the secure link.

27. A method of establishing a secure link between a first machine and multiple services on a second machine, comprising the steps of:

filtering traffic so that traffic from each service is separate;

negotiating and authenticating a Security Association (SA) with at least one filter corresponding to the services and the traffic; and

employing the SA to establish the secure link.

28. A system for establishing a secure link among multiple users on a single machine with a remote machine, comprising:

means for filtering traffic so that traffic from each user is separate;

means for negotiating and authenticating a Security Association (SA) with at least one filter corresponding to the user and the traffic; and

means for employing the SA to establish the secure link.

29. A system of establishing a secure link between a first machine and multiple services on a second machine, comprising:

means for filtering traffic so that traffic from each service is separate;

means for negotiating and authenticating a Security Association (SA) with at least one filter corresponding to the services and the traffic; and

means for employing the SA to establish the secure link.

30. A computer readable medium having stored thereon computer executable components, comprising:

a component to filter traffic between a first machine, having multiple users, and a second machine so that traffic for the first machine is separated in accordance with the respective users; and

a component to generate and associate a Security Association (SA) with at least one filter, corresponding to at least one of the users and the respective traffic, and employs the SA to establish a secure link between the first and second machines.

31. A data packet adapted to be transmitted between at least two processes, comprising:

a first component to filter traffic between a first process, associated with multiple users, and a second process so that traffic for the first process is separated in accordance with the respective users; and

a second component to generate and associate a Security Association (SA) with at least one filter, corresponding to at least one of the users and the respective traffic, and employs the SA to establish a secure link between the first and second processes.

32. A computer readable medium having stored thereon computer executable components, comprising:

a component to filter traffic between a first machine, having multiple services, and a second machine so that traffic for the first machine is separated in accordance with the respective services; and

a component to generate and associate a Security Association (SA) with at least one filter, corresponding to at least one of the services and the respective traffic, and employs the SA to establish a secure link between the first and second machines.

33. A data packet adapted to be transmitted between at least two processes, comprising:

a first component to filter traffic between a first process, associated with multiple services, and a second process so that traffic for the first process is separated in accordance with the respective services; and

a second component to generate and associate a Security Association (SA) with at least one filter, corresponding to at least one of the services and the respective traffic, and employs the SA to establish a secure link between the first and second processes.

34. The data packet of claim 33, wherein at least one of the processes is executed by a distributed processing system.